IN THE CLAIMS

Please amend the claims as follows:

Claim 1 (Currently Amended): An information-processing apparatus ~~used for carrying out a process to decrypt~~ for decrypting encrypted data stored on an information-recording medium, said information-processing apparatus ~~having~~ comprising a plurality of encryption-processing units, each encryption-processing ~~means for~~ unit including said encrypted data stored on said information-recording medium and comprising:

first generating means for generating a first block key Kb1 on the basis of a first seed serving as key generation information set for the ~~each of~~ encryption-processing unit ~~units composing said encrypted data stored on said information-recording medium~~;

acquiring means for acquiring a second seed by ~~carrying out a process to decrypt~~ decrypting an encrypted second seed stored on said information-recording medium on the basis of said generated first block key Kb1;

second generating means for generating a second block key Kb2 by ~~carrying out an encryption process~~ encrypting based on said acquired second seed; and

decrypting means for decrypting said encrypted data stored on said information-recording medium based on said generated second block key Kb2.

Claim 2 (Currently Amended): The information-processing apparatus according to claim 1, said information-processing apparatus ~~having~~ including storage means for storing master-key generation information, wherein ~~said encryption-processing means:~~

master key generating means generates a master key on the basis of said master-key generation information[[;]],

recording key generating means generates ~~two recording keys~~ first recording key K1 and second recording key K2 on the basis of said generated master key and information read out from said information-recording medium[[;]],

said first generating means generates ~~a~~ said first block key Kb1 by ~~carrying out an encryption process~~ encrypting based on said generated first recording key K1 and said first seed[[;]],

said acquiring means acquires ~~a~~ said second seed by ~~carrying out a process to decrypt~~ decrypting ~~an~~ said encrypted second seed stored on said information-recording medium on the basis of said generated first block key Kb1[[;]],

said second generating means generates ~~a~~ said second block key Kb2 by ~~carrying out an encryption process~~ encrypting based on said acquired second seed and said generated second recording key K2[[;]], and

decoding means decodes encrypted data stored on said information-recording medium by ~~carrying out a decryption process~~ decrypting based on said generated second block key Kb2.

Claim 3 (Currently Amended): The information-processing apparatus according to claim 2 wherein ~~said encryption processing means also:~~

unique key generating means generates a first title unique key and a second title unique key on the basis of said master key, a disc ID, which is information read out from said information-recording medium, and two title keys recorded on said information-recording medium[[;]], and

said recording key generating means generates ~~a~~ said first recording key K1 by ~~carrying out an encryption process~~ encrypting based on said first title unique key and first information read out from said information-recording medium[[;]], and generates ~~a~~ said

second recording key K2 by ~~carrying out an encryption process~~ encrypting based on said second title unique key and second information read out from said information-recording medium.

Claim 4 (Currently Amended): The information-processing apparatus according to claim 2 wherein said encryption-processing means also:

unique key generating means generates a first title unique key and a second title unique key on the basis of said master key, a disc ID, which is information read out from said information-recording medium, and one key seed recorded on said information-recording medium[[;]], and

said recording key generating means generates ~~a~~ said first recording key K1 by ~~carrying out an encryption process~~ encrypting based on said first title unique key and first information read out from said information-recording medium[[;]], and generates ~~a~~ said second recording key K2 by ~~carrying out an encryption process~~ encrypting based on said second title unique key and second information read out from said information-recording medium.

Claim 5 (Currently Amended): An information-recording medium drive ~~used for reading~~ configured to read out encrypted data from an information-recording medium and ~~outputting~~ output said encrypted data to an external apparatus, said information-recording medium drive comprising:

an authentication-processing unit ~~for carrying~~ configured to carry out an authentication process with said external apparatus to receive said encrypted data read out from said information-recording medium in order to generate a session key Ks; and

a plurality of encryption-processing units, each encryption-processing ~~means for:~~ unit including said encrypted data stored on said information-recording medium and configured to:

~~generating~~ generate a first block key Kb1 on the basis of a first seed serving as key generation information set for the encryption-processing unit ~~each of encryption-processing units composing said encrypted data stored on said information-recording medium~~[[;]],

~~acquiring~~ acquire a second seed by ~~carrying out a process to decrypt~~ decrypting an encrypted second seed stored on said information-recording medium on the basis of said generated first block key Kb1[[;]], and

~~generating~~ generate output-use encrypted information by ~~carrying out a process to encrypt~~ encrypting data including said second seed on the basis of said session key Ks, wherein said output-use encrypted information obtained as a result of said process to encrypt data including said second seed on the basis of said session key Ks is output through an interface.

Claim 6 (Currently Amended): The information-recording medium drive according to claim 5 wherein ~~said~~ each encryption-processing unit is further configured to ~~means also~~:

~~generates~~ generate a master key on the basis of master-key generation information held by said information-recording medium drive;

~~generates~~ generate two recording keys K1 and K2 on the basis of said master key and information read out from said information-recording medium;

~~generates~~ generate ~~a~~ the first block key Kb1 by carrying out an encryption process based on said generated first recording key K1 and said first seed;

~~acquires~~ acquire ~~a~~ the second seed by ~~carrying out a process to decrypt an~~ decrypting the encrypted second seed stored on said information-recording medium on the basis of said generated first block key Kb1;

~~generates~~ generate the output-use encrypted information by encrypting data including said second seed and said second recording key K2 on the basis of said session key Ks; and

~~outputs~~ output said output-use encrypted information including said second seed and said second recording key K2 through an interface.

Claim 7 (Currently Amended): An information-processing apparatus ~~used~~ for ~~carrying out a process to decrypt~~ decrypting encrypted data received from an external apparatus through a data input interface, said information-processing apparatus comprising:

an authentication-processing unit for carrying out an authentication process with said external apparatus outputting said encrypted data in order to generate a session key Ks; and

an encryption-processing unit for:

acquiring a seed used as key generation information and a recording key by ~~carrying out a process~~ decrypting, based on said session key, ~~to decrypt~~ encrypted information received through said data input interface[[;]],

generating a block key to be used as a decryption key for decryption of encrypted data by ~~carrying out an encryption process~~ encrypting, based on said seed and said recording key[[;]], and

~~carrying out a process~~ decrypting, based on said block key, ~~to decrypt~~ said encrypted data.

Claim 8 (Currently Amended): An information-recording medium drive ~~used~~ for reading out encrypted data from an information-recording medium and outputting said

encrypted data to an external apparatus, said information-recording medium drive ~~having a configuration~~ comprising:

an authentication-processing unit for carrying out an authentication process with said external apparatus to receive said encrypted data read out from said information-recording medium in order to generate a session key Ks; and

a plurality of encryption-processing units including said encrypted data stored on said information-recording medium, each encryption-processing unit comprising ~~means for~~:

means for generating a block key on the basis of a seed serving as key generation information set for ~~each of~~ the encryption-processing ~~units~~ unit ~~composing said encrypted data stored on said information-recording medium~~;

means for acquiring decrypted data by ~~carrying out a process to decrypt~~ decrypting said encrypted data stored on said information-recording medium on the basis of said generated block key; and

means for generating output-use encrypted information by ~~carrying out a process to encrypt~~ encrypting said decrypted data on the basis of said generated session key Ks,

wherein said output-use encrypted information obtained as a result of said ~~process to encrypt~~ encrypting of said decrypted data on the basis of said session key Ks is output through an interface.

Claim 9 (Currently Amended): ~~An~~ A method of manufacturing an information-recording medium used for storing encrypted data, said method comprising ~~information-recording medium comprising a configuration for storing~~:

generating, outside the information-recording medium, a first seed serving as key generation information set for each of encryption-processing units composing said encrypted data;

storing said first seed in the information-recording medium;

generating, outside the information-recording medium, a second seed serving as key generation information encrypted on the basis of a first block key [[Kb2]] Kb1 generated on the basis of said first seed;

storing said second seed in the information-recording medium; ~~and~~

generating, outside the information-recording medium, an encrypted content encrypted on the basis of a second block key [[Kb1]] Kb2 generated on the basis of said second seed; and

storing said encrypted content in the information-recording medium.

Claim 10 (Currently Amended): The ~~information-recording medium~~ method according to claim 9 wherein said first seed is stored inside control information set for each of encryption-processing units whereas said second seed is stored as encrypted information in a user-data area outside said control information.

Claim 11 (Currently Amended): The ~~information-recording medium~~ method according to claim 9 wherein said first seed is stored in a user-data area as unencrypted data whereas said second seed is stored in said user-data area as encrypted data.

Claim 12 (Currently Amended): The ~~information-recording medium~~ method according to claim 9 wherein said encrypted data is a transport stream packet, said first seed is stored inside control information for a plurality of transport stream packets, and said

second seed is stored as encrypted information inside one of said transport stream packets in a user-data area outside said control information.

Claim 13 (Currently Amended): The ~~information-recording medium~~ method according to claim 9 wherein said first seed is stored inside a transport stream packet in a user-data area as unencrypted data whereas said second seed is stored as encrypted information inside said transport stream packet in said user-data area.

Claim 14 (Currently Amended): An information-processing method ~~used~~ for ~~carrying out a process to decrypt~~ decrypting encrypted data stored on an information-recording medium, said information-processing method comprising ~~the steps of~~:

generating a first block key Kb1 on the basis of a first seed serving as key generation information set for each of a plurality of encryption-processing units ~~composing~~ including said encrypted data stored on said information-recording medium;

acquiring a second seed by ~~carrying out a process to decrypt~~ decrypting an encrypted second seed stored on said information-recording medium on the basis of said generated first block key Kb1;

generating a second block key Kb2 based on said acquired second seed; and

decrypting said encrypted data stored on said information-recording medium by ~~carrying out a decryption process~~ decrypting, based on said generated second block key Kb2.

Claim 15 (Currently Amended): The information-processing method according to claim 14, said information-processing method further comprising ~~having the steps of~~:

generating a master key on the basis of master-key generation information read out from storage means;

generating two recording keys K1 and K2 on the basis of said generated master key and information read out from said information-recording medium;

generating [[a]] said first block key Kb1 by ~~carrying out an encryption process~~ encrypting, based on said generated first recording key K1 and said first seed;

acquiring [[a]] said second seed by carrying out a process to decrypt an encrypted second seed stored on said information-recording medium on the basis of said generated first block key Kb1;

generating [[a]] said second block key Kb2 by ~~carrying out an encryption process~~ encrypting, based on said acquired second seed and said generated second recording key K2; and

decrypting said encrypted data stored on said information-recording medium by ~~carrying out a decryption process~~ decrypting, based on said generated second block key Kb2.

Claim 16 (Currently Amended): The information-processing method according to claim 15, said information-processing method further comprising ~~having the steps of~~:

generating a first title unique key and a second title unique key on the basis of said master key, a disc ID, which is information read out from said information-recording medium, and two title keys recorded on said information-recording medium;

generating [[a]] said first recording key K1 by ~~carrying out an encryption process~~ encrypting, based on said first title unique key and first information read out from said information-recording medium; and

generating [[a]] said second recording key K2 by ~~carrying out an encryption process~~ encrypting, based on said second title unique key and second information read out from said information-recording medium.

Claim 17 (Currently Amended): The information-processing method according to claim 15, said information-processing method further comprising ~~having the steps of~~:

generating a first title unique key and a second title unique key on the basis of said master key, a disc ID, which is information read out from said information-recording medium, and one key seed recorded on said information-recording medium;

generating [[a]] said first recording key K1 by ~~carrying out an encryption process~~ encrypting, based on said first title unique key and first information read out from said information-recording medium; and

generating [[a]] said second recording key K2 by ~~carrying out an encryption process~~ encrypting, based on said second title unique key and second information read out from said information-recording medium.

Claim 18 (Currently Amended): An information-processing method used for reading out encrypted data from an information-recording medium and outputting said encrypted data to an external apparatus, said information-processing method comprising ~~the steps of~~:

carrying out an authentication process with said external apparatus to receive said encrypted data read out from said information-recording medium in order to generate a session key Ks; and

generating, outside said information-recording medium, a first block key Kb1 on the basis of a first seed serving as key generation information set for each of encryption-processing units composing said encrypted data stored on said information-recording medium;

acquiring a second seed, outside said information-recording medium, by ~~carrying out a process to decrypt~~ decrypting an encrypted second seed stored on said information-recording medium on the basis of said generated first block key Kb1;

generating output-use encrypted information by ~~carrying out a process to encrypt~~ encrypting data including said second seed on the basis of said session key Ks; and

outputting said output-use encrypted information obtained as a result of ~~said process to encrypt~~ encrypting data including said second seed on the basis of said session key Ks through an interface.

Claim 19 (Currently Amended): The information-processing method according to claim 18, said information-processing method further comprising ~~having the steps of~~:

generating a master key on the basis of master-key generation information held by an information-recording medium drive;

generating two recording keys K1 and K2 on the basis of said master key and information read out from said information-recording medium;

generating [[a]] said first block key Kb1 by ~~carrying out an encryption process~~ encrypting, based on said generated first recording key K1 and said first seed;

acquiring [[a]] said second seed by ~~carrying out a process to decrypt~~ decrypting an encrypted second seed stored on said information-recording medium on the basis of said generated first block key Kb1;

generating said output-use encrypted information by encrypting data including said second seed and said second recording key K2 on the basis of said session key Ks; and

outputting said output-use encrypted information including said second seed and said second recording key K2 through an interface.

Claim 20 (Currently Amended): An information-processing method used for carrying out a process to decrypt encrypted data received from an external apparatus through a data input interface, said information-processing method comprising ~~the steps of~~:

carrying out an authentication process with said external method outputting said encrypted data in order to generate a session key Ks;

acquiring a seed used as key generation information and a recording key by ~~carrying out a process~~ decrypting, based on said session key, ~~to decrypt~~ encrypted information received through said data input interface;

generating a block key to be used as a decryption key for decryption of encrypted data by ~~carrying out an encryption process~~ encrypting, based on said seed and said recording key; and

~~carrying out a process based on said block key to decrypt~~ decrypting encrypted data.

Claim 21 (Currently Amended): An information-processing method used for reading out encrypted data from an information-recording medium and outputting said encrypted data to an external apparatus, said information-processing method comprising ~~the steps of~~:

carrying out an authentication process with said external method to receive said encrypted data read out from said information-recording medium in order to generate a session key Ks;

generating a block key on the basis of a seed serving as key generation information set for each of a plurality of encryption-processing units ~~composing~~ including said encrypted data stored on said information-recording medium;

acquiring decrypted data by ~~carrying out a process to decrypt~~ decrypting encrypted data stored on said information-recording medium on the basis of said generated block key;

generating output-use encrypted information by ~~carrying out a process to encrypt~~ encrypting said decrypted data on the basis of said generated session key Ks; and

outputting said output-use encrypted information obtained as a result of said process to encrypt said decrypted data on the basis of said session key Ks through an interface.

Claim 22 (Currently Amended): A computer-readable storage medium configured to store a program, which, when executed, performs a method of decrypting ~~to be executed for carrying out a process to decrypt~~ encrypted data stored on an information-recording medium, said ~~computer program~~ method comprising ~~the steps of~~:

generating a first block key Kb1 on the basis of a first seed serving as key generation information set for each of encryption-processing units composing said encrypted data stored on said information-recording medium;

acquiring a second seed by ~~carrying out a process to decrypt~~ decrypting an encrypted second seed stored on said information-recording medium on the basis of said generated first block key Kb1;

generating a second block key Kb2 based on said acquired second seed; and

decrypting said encrypted data stored on said information-recording medium by ~~carrying out a decryption process~~ decrypting, based on said generated second block key Kb2.